Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(12)

<SYSTEM> <VERSION>

ANALYSUNDERLAG *IDENTIFIERA* (AU-I)

Innehåll

1 Basfakta 6
1.1 Giltighet och syfte 6
1.2 Revisionshistorik 6
1.3 Terminologi och begrepp 6
1.4 Bilageförteckning 6
1.5 Referenser 6
2 Granskning av indata från FM och FMV 7
2.1 Granskning av indata från FM 7
2.2 Granskning av styrande dokument från FMV 7
3 Säkerhetsanalys 8
3.1 Skyddsvärda informationstillgångar 8
3.1.1 Sekretess 8
3.1.2 Riktighet 8
3.1.3 Tillgänglighet 9
3.1.4 Spårbarhet 9
3.2 Regelverk som IT-system omfattas av 9
3.3 Regelverk som behandlade uppgifter omfattas av 9
4 Användningsfall 10
4.1 Informationsflöde och informationsklassificering 10
4.2 Externa gränsytor 11
4.3 Exponeringsanalys 11
4.4 Hotanalys 12

Mallinformation 18FMV6730-2:1.1

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Mall för AU-I	DAOLO

Mallinstruktion och omfattning av analysunderlag *Identifiera*

AU-I syftar till att få fram så mycket information kring verksamheten ur ett säkerhetsperspektiv att realiserbarhet ur ett informationssäkerhetsperspektiv för aktuellt IT-system kan bedömas i ett tidigt skede. Informationen inhämtas från Försvarsmakten alternativt fås fram genom analysarbete av FMV. Underlaget ska också skapa förutsättningar för *Definiera* att leverera ackrediterbart IT-system med önskad förmåga till Försvarsmakten.

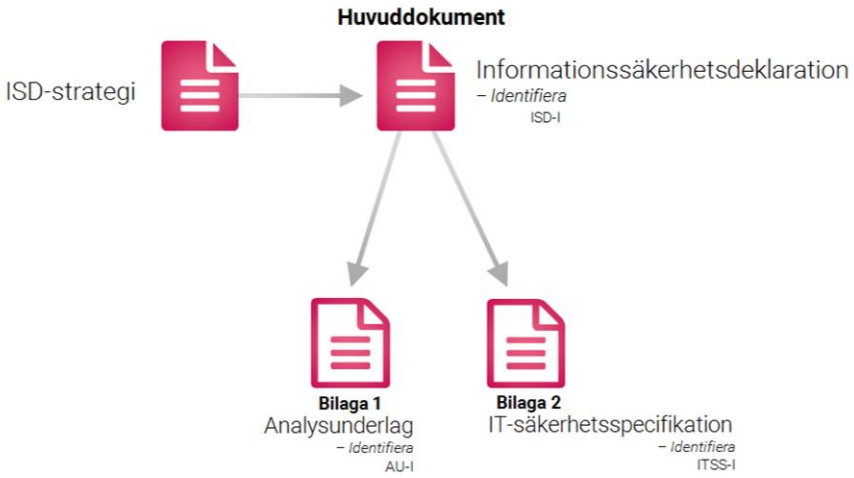
Sidorna från innehållsförteckning till kapitel 1 Basfakta innehåller hjälp och metodbeskrivning för bilaga 1 till Informationssäkerhetsdeklaration *Identifiera*. Dessa ska raderas innan dokumentet färdigställs.

- Instruktionen om vad som ska stå under varje rubrik anges under respektive rubrik. Gulmarkerad text ska raderas innan dokumentet färdigställs.
- Text utan gulmarkering kan användas också i det färdigställda dokumentet.
- Ersätt *Systemnamn* med ackrediteringsobjektets namn.

Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av Analysunderlag *Identifiera*

Informationssäkerhetsdeklaration *Identifiera* består av ett huvuddokument nedan benämnt ISD-I och två bilagor Analysunderlag (AU-I) och IT-SäkerhetsSpecifikation ITSS-I. AU-I innehåller relevanta analyser avseende informationssäkerhetsaspekten ur ett verksamhetsperspektiv. Denna mall utgör bilaga 1 AU-I.



Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Identifiera

Följande analyser ska stödja realiserbarhetsbedömningen i *Identifiera* framtagning av ovan nämnda information:

- Granskning av indata från FMs säkerhetsmålsättningsarbete i form av verksamhetsanalys, regelverksanalys och säkerhetsanalys.Innehåll och kvalitet i de underlag som ska användas som kravkällor analyseras. Vid behov kan FM kravunderlag behöva kompletteras med följande analyser:
    - Säkerhetsanalys - Identifiering och analys av skyddsvärda tillgångar som ligger till grund för framtagning av användningsfall. Identifiera vilka skyddsvärda tillgångar som finns i verksamheten för att identifiera information om verksamheten som kan bli dimensionerande för informationssäkerhetsaspekterna. Detta ligger till grund vid framtagning av användningsfall.
    - Användningsfall –scenariobeskrivning av IT-systemets tilltänkta användning är ett exempel på hur information kring verksamheten kan tas fram. Användningsfallen beskriver IT-systemets kontext såsom hur det ska användas och i vilken miljö. Identifierade användningsfall ska vara dimensionerande ur ett informations-säkerhetsperspektiv. Input till användningsfall kan t.ex. hämtas från systemmålsättning, ISD-strategi, intervjuer/gruppövningar med verksamheten etc.
    - Hotanalys – beskriver vilka hot som verksamheten ser att IT-systemet kan komma att påverkas av.
    - Informationsflödet i användningsfallen samt och informationsklassificeringRegelverksanalys avseende aktuella författningar som är relevanta förutom det som hanterar riket säkerhet OSL 2009:400 15 kap §2 vilka hanteras inom ramen för MUST KSF.
    - Exponeringsanalys. Exponeringsanalysen beskriver exponering av den information som ska skyddas i verksamheten och det aktuella IT-systemet. Exponering kan vara antal användare, fysiskt skydd, externa/interna gränsytor mm. Typ av exponering påverkar behov av säkerhetslösning och kan påverka bedömningen av ackrediterbarhet.

Slutsatser från analyserna dokumenteras i Huvuddokumentet ISD-I och resultatet från analyserna i form av krav dokumenteras i bilaga 2 - ITSS-I.

Att tänka på i arbetet med framtagning av AU-I

Arbetet i *Identifiera* utgår från verksamhetens perspektiv för IT-systemets hela livscykel. Indata till analyserna inhämtas från:

- ISD-strategi
- Försvarmaktens säkerhetsmålsättningsarbete

Analyser för att komplettera Försvarsmaktens säkerhetsmålsättningsarbete kan behöva göras. Bedömning av rätt informationsklass på informationen som ska lagras, kommuniceras och hanteras kan spara både pengar och tid. Bedömningen ska göras av FM men om inte det är gjort måste det göras i *Identifiera*. Att klassa information högre än vad som faktiskt krävs kan driva höga kostnader och processer runt utvecklingen är omfattande tex i form krav på assurans och även på säkerhetsfunktionerna i sig.

Exponeringsanalys är en viktig aktivitet. Att få ner exponeringen på IT-systemet påverkar kravnivå som i sin tur påverkar kostnader och tid.

Hot mot verksamheten och dess konsekvenser identifieras i hotanalysen för att få fram verksamhetens sårbarheter. En regelrätt riskanalys går dock inte att genomföra innan designarbetet har genomförts till fullo. Verksamhetens sårbarheter omsätts sedan till tillkommande säkerhetskrav.

I det fall IT-systemet utgörs av system av system ska detta framgå, information kring det kan hämtas från ISD-strategin alt. från huvuddokumentet ISU-I där aktuellt IT-system är definierat.

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är Analysunderlag *Identifiera* (AU-I) för <System> <version> inför FMV VHL S2-beslut.

Analysunderlaget för *Identifiera* (AU-I) har fokus på att få fram informationssäkerhetskraven utifrån verksamhetens perspektiv. Analyserna är av vital betydelse för att få rätt indata och skapa förutsättningar för att bedöma ackrediterbarhet i tidigt stadie i utvecklingen och därmed kunna leverera ackrediterbara IT-system.

Analysunderlaget för *Identifiera* omfattar huvudsakligen Försvarsmaktens säkerhetsmålsättningsarbete. Vid avsaknad av eller brister i information från Försvarsmakten genomförs analyserna i *Identifiera*. resultatet dokumenteras som krav i bilaga 2 ITSS-I.

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

Följande tabell innehåller specifika begrepp som gäller för detta dokument. En generell lista återfinns i ref [1].

Term (förkortning)	Definition	Källa	Kommentarer/ Anmärkningar
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	

Tabell 2 - Terminologi och begrepp i detta dokument

1.4 Bilageförteckning

Detta dokument har inga bilagor.

1.5 Referenser

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] ISD Begrepp och förkortningar	18FMV6730-8:1.1	1
[2] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>
[3] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>

Tabell 3 - Referenser

2 Granskning av indata från FM och FMV

2.1 Granskning av indata från FM

- Identifiera FM krav dokument och förteckna dessa i ITSS-I
- Granska FM kravdokument med avseende på innehåll och kvalitet i kravställningen.
- Säkerställ giltighet på FM kravdokument
- Klargör om komplettering av FM indata behövs, och bedöm i så fall omfattning och tidsåtgång
- Identifiera tidigare inriktningar och beslut, och huruvida dessa fortfarande gäller

2.2 Granskning av styrande dokument från FMV

- Finns en tidigare ISD-Strategi
- Identifiera FMV styrande dokument och förteckna dessa i ITSS-I
- Säkerställ giltighet på FMV styrande dokument
- Identifiera tidigare inriktningar och beslut, och huruvida dessa fortfarande gäller

3 Säkerhetsanalys

Finns Säkerhetsanalys från Försvarsmaktens säkerhetsmålsättningsarbete ska den informationen användas alt kompletteras vid behov. Finns inte informationen från Försvarsmakten kan den erhållas genom följande aktiviteter:

- Identifiera vilka skyddsvärda tillgångar som finns i verksamheten.
- För identifierade skyddsvärda tillgångar görs även en informationsklassificering och bedömning konsekvensnivå för de skyddsvärda tillgångarna. Det är viktigt att informationsklassningen sker med motivering och konsekvensbedömning avseende kostnad kontra funktionalitet. Fel satt informationsklassificering kan vara kostnadsdrivande och påverka tidsplan.
- Skyddsvärda tillgångar värderas med utgångspunkt från sekretess, tillgänglighet, riktighet och spårbarhet.
- För uppgifter som omfattas av sekretess enligt OSL (2009:400) ska en konsekvensbedömning göras.
- Analysera vilka prioriteter verksamheten har. Ansvarig i verksamheten måste delta i denna bedömning. Resultatet dokumenteras i tabellen som finns i kapitel 3.1 och blir sedan drivande i framtida arbete. Prioritering av skyddsvärda tillgångar utförs för att verksamhetens perspektiv ska komma fram och är kopplat till förmåga och uppgift. Prioritering tillsammans med informationens klassning blir dimensionerande i arbetet med utvecklingen av IT-systemet.
- Informationsklassificeringen av de skyddsvärda tillgångarna används sedan i kapitel 4.1 där den konkretiseras till specifika användningsfall och informationsflöden.
- Informationstillgångar, personuppgifter och klassning av materiel är exempel på skyddsvärda tillgångar. Fyll på med egna rubriker efter vad som är tillämpligt för systemet i fråga.
- Författningar som IT-systemet omfattas av.

3.1 Skyddsvärda informationstillgångar

Tabellerna nedan redovisar informationsklassificering för delsystem ingåendes i <*System*>. En tabell för informationssäkerhetsområdena sekretess, riktighet, tillgänglighet och spårbarhet. Kolumnen ”Informationsmängd” anger vilken typ av information som avses och i kolumnen ”Prioritet” anges verksamhetens prioritering av de skyddsvärda tillgångarna. I ”Kommentar” ges förtydliganden av klassificeringen eller annan relevant information.

3.1.1 Sekretess

Information	Prioritet	Kommentar

Tabell 4 – Skyddsvärda tillgångar med avseende på sekretess

3.1.2 Riktighet

Information	Prioritet	Kommentar

Tabell 5 – Skyddsvärda tillgångar med avseende på riktighet

3.1.3 Tillgänglighet

Information	Prioritet	Kommentar

Tabell 6 – Skyddsvärda tillgångar med avseende på tillgänglighet

3.1.4 Spårbarhet

Information	Prioritet	Kommentar

Tabell 7 – Skyddsvärda tillgångar med avseende på spårbarhet

3.2 Regelverk som IT-system omfattas av

Detta avsnitt beskriver de regelverk som IT-systemet omfattas av vid behandling av vissa uppgifter tex personuppgifter. Ange då även vilka delsystem som omfattas.

ID	Regelverk	Benämning

Tabell 8 – Regelverk som IT-systemet omfattas av

3.3 Regelverk som behandlade uppgifter omfattas av

Detta avsnitt beskriver de regelverk som behandlade uppgifter omfattas av.

ID	Regelverk	Benämning

Tabell 9 – Regelverk som behandlade uppgifter omfattas av

4 Användningsfall

Finns nedanstående information i underlag från Försvarsmaktens säkerhetsmålsättningsarbet ska den användas. Finns inte informationen från Försvarsmakten kan den erhållas genom aktiviteter beskrivna i kapitel 4:
Syftet med användarfall är att ge en rimlig uppfattning om:

- Vilka driftmiljöer som kan tänkas bli aktuella.
- Vilka hot som bör belysas i en separat analys.
- Vilka regelverksområden som kan komma att påverkas i och med behovet av en viss informationsstruktur.
- Vilka säkerhetsdomäner som passeras, identifiera om det finns en risk att information med olika informationssäkerhetsklass möts.
- Övergripande beskrivning av syftet med verksamheten vid behov.

Förslag på genomförande avseende användningsfallen är:

- Hämta information från säkerhetsanalysen såsom bedömning av konsekvensen avseende oönskad spridning av sekretess, tillgänglighetsförlust och oönskad förändring för respektive tillgång samt prioriteringen av tillgången.
- Identifiera dimensionerande användningsfall och stödprocesser med utgångspunkt från tillgångarna. Användningsfallen utgörs av en aktivitet eller en sekvens av aktiviteter som en aktör utför inom en verksamhet/ett system för att uppfylla en specifik förmåga.
- Identifiera informationsflödet i användningsfallen, dokumentera i kapitel 4.1.
- Genomför informationsklassificering, dokumentera i kapitel 4.1
- Genomför exponeringsanalys, dokumentera i kapitel 4.3
- Genomför hot med avseende på verksamhetens sårbarhet med utgångspunkt användningsfall och identifierade informationsflöden, dokumentera i kapitel 4.4.

Aktörer till användningsfallen kan dels vara aktuella roller som ska verka i systemet men även aktörer som system kan vara aktuella att identifiera.

Ur användningsfallen extraheras verksamhetskrav som förs in i kravtabellen i bilaga 2-ITSS-I.

4.1 Informationsflöde och informationsklassificering

I detta kapitel beskrivs och illustreras informationsflödet på en övergripande nivå.

- I samband med beskrivning av informationsflöde och gränsytor till andra verksamheter/system placeras även värden för informationsklassning ut.
- Input till detta informationsflöde erhålls ur användningsfallen i kapitel 4.1.
- I verksamheten kan resultatet av informationsklassificering ändras utifrån den verksamhet som bedrivs just där. Konkretiseringen kan ske utifrån aspekter som t.ex. tid och rum. Denna aktivitet är viktig resultatet påverkar kostnader, funktionalitet och tid.
- Informationsklassningen i analysunderlaget blir sedan stöd för designfasen.

Användningsfall	Information	Klassificering	Ingående delsystem

Tabell 10 – Informationsflöde och -klassificering

4.2 Externa gränsytor

- Input till externa gränsytor erhålls ur användningsfallen i kapitel 4.2 ovan.
- Vilken information utbyts med andra system/verksamheter?
- Vilka andra IT-system/verksamheter kan ställa krav på detta IT- system (funktion, information)?
- Vilka krav ställer detta IT-systemsystem på andra IT-system/verksamheter (funktion, information)?
- Input till informationsklassificering kan erhållas ur säkerhetsanalysen kapitel
- Gränsytor kan finnas beskrivet i systemmålsättning eller i annan verksamhetsdokumentation (processer, rutiner, organisationsscheman etc.)

Tabellen nedan anger externa gränsytor och informationsflöde till andra verksamheter/IT-system. Kolumnen ”Verksamhet/System” anger vilken verksamhet/system som information utbyts med. Kolumnen ”Information” anger vilken slags information som utbyts och i kolumnen ”Klassificering” anges informationsklassificering.

Verksamhet/system	Information	Klassificering	Kommentar

Tabell 11 – Externa gränsytor

4.3 Exponeringsanalys

- Informationen i kapitlet ska bl.a. användas för att skapa en uppfattning av exponeringsnivå vid bedömningen av vilka säkerhetskrav som ska tillämpas för IT-systemet utifrån MUST KSF.
- Med exponeringsnivå avses bedömningen av hur exponerat systemet är avseende någon aktörs möjlighet att påverka systemet. Denna möjlighet kan vara såväl fysisk, d.v.s. att någon kommer åt den tekniska utrustning som utgör systemet, som logisk via systemets olika gränssnitt.
- Input till detta kapitel kan erhållas ur ovanstående kapitel Användningsfall, Informationsflöde inom systemet, Externa gränsytor till andra verksamheter eller system.
- I kapitlet ska följande beskrivas:
    - Vilka resurser för skydd av verksamhet och IT-systemet och informationen i IT-systemet som finns t.ex. i form av fysiskt skydd
    - Om IT-systemet ska användas nationellt eller internationellt
    - Om IT-systemet ska användas i fred, kris eller krig
    - Exponering från t.ex. personer
    - Exponering från t.ex. informationsutbyte. Med informationsutbyte avses allt utbyte av information med andra IT-system, vare sig det sker över elektroniskt kommunikationsnät eller med flyttbara lagringsmedia.
    - Exponering från såväl fysiska som logiska aspekter.

4.4 Hotanalys

Hotanalysen genomförs på användningsfallen alt på annan beskriven verksamhet. Hotanalysen genomförs för att få fram verksamhetens sårbarheter på övergripande nivå för att kunna få fram verksamhetskrav avseende informationssäkerhet.
Hoten kan identifieras utifrån användningsfallen och förtecknas nedan ett och ett samt bearbetats enligt följande:

- Hotets kod (Se = sekretess, Ri = riktighet, Ti = tillgänglighet, Ge = generellt) samt ett löpnummer
- Rubrik/Beskrivning av hotet
- Beskrivning av scenario/händelseförloppet där scenariot utgör en beskrivning av hur hotet kan inträffa. I scenariobeskrivning exemplifieras hotrubriken genom att svara på:
  - Hur inträffar scenariot?
  - När inträffar scenariot?
  - Var inträffar scenariot?
  - Vilken typ av fysisk miljö inträffar scenariot i?
  - Vem utför scenariot?
- Beskrivning av skadan som uppstår (konsekvens)

Hot ID:	
Beskrivning:	
Scenario:	
Konsekvens:	

Tabell 12 – Hotanalys